

Н. А. ВЕРЗУН, А. И. ВОРОБЬЁВ, Е. Д. ПОЙМАНОВА

МОДЕЛИРОВАНИЕ ПРОЦЕССА ПЕРЕДАЧИ ИНФОРМАЦИИ С РАЗГРАНИЧЕНИЕМ ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ

Рассматривается информационная сеть предприятия сервиса с использованием централизованного устройства контроля доступа для организации санкционированного доступа пользователей к ресурсам сети. Предложена математическая модель сети и метод расчета вероятностно-временных характеристик процессов передачи информации.

Ключевые слова: информационная сеть, ресурсы сети, устройство контроля доступа, иллюз контроля доступа, математическая модель сети, вероятностно-временные характеристики процессов передачи информации.

Введение. Одним из немаловажных факторов, влияющих на эффективность бизнес-проектов, является, без сомнения, грамотная организация информационного взаимодействия подразделений предприятия [1, 2].

Вместе с тем используемые на предприятии информационные системы при неправильном их развитии могут стать уязвимым местом процесса функционирования предприятия в целом [3]. При этом следует учитывать, что внедрение информационных технологий, необходимых для поддержания бизнес-процесса, наряду с предоставлением новых возможностей и преимуществ, содержит, однако, и определенные угрозы. Используемые в настоящее время методы передачи, обработки и накопления информации связаны с появлением внутренних и внешних угроз, т.е. с возможностью потери, искажения и раскрытия данных, принадлежащих пользователям [4].

Для современного уровня развития информационных систем предприятий сферы сервиса характерно, с одной стороны, значительное увеличение объемов информации, хранимой, обрабатываемой, передаваемой в рамках корпоративной системы. Так, по оценкам специалистов, 70—90 % интеллектуальной собственности компаний хранятся в цифровом виде — в текстовых файлах, таблицах, базах данных [4]. С другой стороны, наблюдается расширение круга пользователей, имеющих непосредственный доступ к информационным ресурсам и сервисам, что ведет к увеличению числа внутренних, преднамеренных или случайных, попыток вмешательства в информационную структуру предприятия [5].

Именно поэтому для защиты интеллектуального капитала компании от внутренних угроз представляется актуальным внедрение и использование в системе управления информационной сетью предприятия аппарата разграничения прав доступа пользователей к ее ресурсам. Проблема санкционированного доступа пользователей к информационным ресурсам может быть решена путем применения централизованного устройства управления доступом. В данном случае решение о доступе каждого конкретного пользователя к информационным ресурсам сети предприятия принимает устройство контроля доступа.

Использование централизованного устройства контроля доступа позволит обеспечить конфиденциальность информации, т.е. ее защиту от несанкционированного просмотра лицами, не имеющими на это право, доступность информации и ее целостность.

В настоящей статье предлагается вариант структуры информационной сети с централизованным устройством контроля доступа к ее ресурсам.

Структура информационной сети. В состав сети, структура которой представлена на рис. 1, входят N рабочих станций и централизованное устройство контроля доступа (УКД). Рабочие станции подключаются к сети через шлюзы контроля доступа (ШКД). Процесс доступа пользователей к информационным ресурсам корпоративной сети осуществляется следующим образом: перед началом сеанса связи (обращением к ресурсам сети) рабочие станции через ШКД отправляют запрос на его разрешение УКД, которое принимает решение о доступе и отправляет ответ-разрешение (либо ответ-запрет) на создание сеанса связи, основываясь на определенной политике безопасности, а также на текущем состоянии системы [6, 7]. УКД может также давать дополнительные команды управления рабочим станциям. В общем случае УКД может рассматриваться как рабочее место администратора сети.

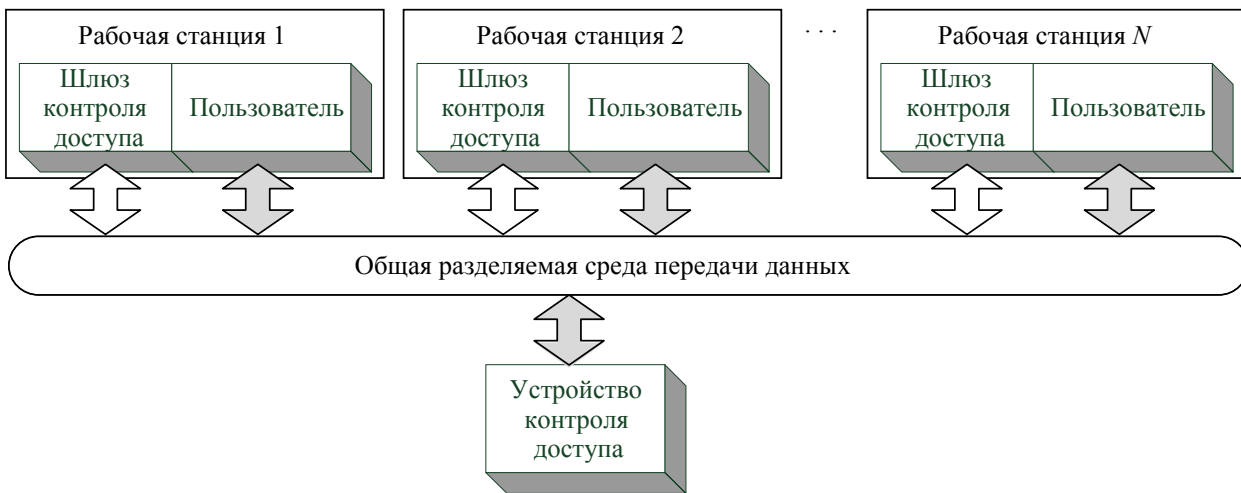


Рис. 1

Все передающие элементы сети можно разбить на три логические группы, т.е. данная сеть представляет собой совокупность 3 подсетей:

- 1 — подсеть пользователей (П),
- 2 — подсеть передачи запросов от ШКД к УКД (ШКД),
- 3 — подсеть передачи ответов от УКД к ШКД (УКД).

Рассмотрим комбинированный метод разделения общего канала передачи данных: между подсетями используется временное разделение — интервалы однократного доступа подсетей (рис. 2), а внутри подсетей П и ШКД — случайный синхронный доступ (ССД). Подсеть УКД состоит из одного передающего элемента и, таким образом, работает в режиме временного разделения канала.

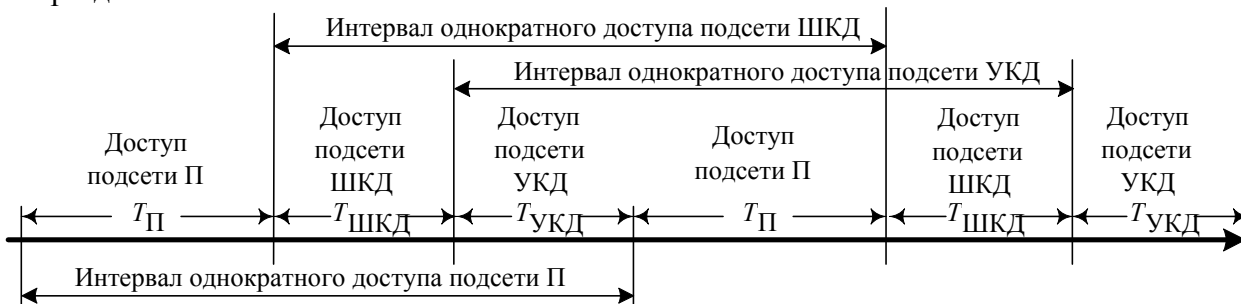


Рис. 2

В отличие от модели, предложенной в работе [8], построим модель в дискретном времени. На вход станции подсети П поступает бернуллиевский поток пакетов данных с интенсивностью $\lambda_{иП}$ на интервалах $T_0 = 1/V_c$, где V_c — скорость передачи сигналов в среде, бит/с. Аналогично и для подсетей ШКД и УКД предположим входные потоки пакетов (запросов и ответов) бернуллиевскими с интенсивностями $\lambda_{иШКД}$ и $\lambda_{иУКД}$ на интервалах T_0 .

Формирование кадров для передачи осуществляется с применением служебных полей: преамбулы длиной $r_{пр}$ разрядов, флага — $r_{ф}$, адреса — r_a , управления — r_y , контрольных разрядов — $r_{кр}$ и информационной части пакета k_i ; здесь и далее $i = \overline{\text{ШКД, УКД, П}}$.

Рассмотрим для передачи всех типов кадров вариант использования алгоритма РОС-ОЖ (решающей обратной связи с ожиданием), предусматривающего применение положительных или отрицательных квитанций длиной $n_{кв}$. Длительность временных окон для передачи кадров-запросов ШКД — $T_{ШКД}$, кадров-ответов УКД — $T_{УКД}$ и пользовательских кадров — $T_{П}$ определяется следующим образом:

$$T_i = c_i V_c^{-1}, \quad c_i = n_i + n_{кв} + t_d V_c + 4 \cdot 10^{-6} D V_c \text{ — для „шины“; } n_i = r_{пр} + r_{ф} + r_a + r_{кр} + r_y + k_i, \quad (1)$$

где n_i — длина кадра, t_d — время декодирования кадров и квитанции; D — длина канала передачи данных, км.

Математическая модель сети. Математическая модель сети может быть представлена совокупностью моделей подсетей, входящих в ее состав [9, 10]. Каждая подсеть представляется системой массового обслуживания $M/G/1$ в дискретном времени на интервалах T_0 .

Подсеть пользователей. Кадры, переданные пользователем, считаются обслуженными при соблюдении следующих условий:

- в сообщениях не обнаружено ошибки в результате применения помехоустойчивого кодирования, вероятность чего обозначается как Q_{ki} ;
- отсутствуют мешающие воздействия станций других пользователей, т.е. нет конфликтов при передаче, вероятность чего обозначается как Q_{mi} ;
- разрешен доступ станции к сети с вероятностью Q_d (в соответствии с протоколом ССД).

Если перечисленные условия не выполняются, доставка всех типов кадров повторяется. Так как используется временное разделение канала между подсетями, то интервал однократной передачи кадров в сети постоянный и равен $C = c_{П} + c_{ШКД} + c_{УКД}$, где $c_{П}$, $c_{ШКД}$ и $c_{УКД}$ — длительности временных окон соответственно для передачи кадров пользователей, запросов ШКД и ответов УКД в интервалах T_0 — определяются по формулам (1). Выражения для z -преобразования рядов распределения (z -прр) интервалов однократной передачи для всех подсетей будут иметь вид

$$g_{si}(z) = z^{-C}, \quad (2)$$

а z -прр интервала обслуживания при передаче информации в подсети П определяется как

$$g_{П}(z) = \frac{Q_{cП}}{z^C - P_{cП}}, \quad Q_{cП} = Q_d Q_{кП} Q_{mП}, \quad P_{cП} = 1 - Q_{cП}; \quad Q_{кП} = (1 - p)^{n_{П}}, \quad Q_{mП} = (1 - Q_d \Theta_{П})^{N-1}, \quad (3)$$

где $n_{П}$ — длина пользовательского кадра, $\Theta_{П}$ — вероятность занятости буфера станции пользователя, p — вероятность ошибки в среде передачи; z -прр времени задержки при передаче информации в подсетях

$$f_{qi}(z) = \frac{(1 - \Theta_i)(1 - z)g_i(z)}{1 - zp_{ni} - q_{ni}z g_i(z)}, \quad q_{ni} = \lambda_{ni} T_0, \quad p_{ni} = 1 - q_{ni}, \quad (4)$$

где q_{ni} — параметры входных потоков.

Подсеть ШКД. Кадры-запросы от ШКД к УКД на разрешение сеанса передачи считаются обслуженными, если не обнаружено ошибки, не было конфликтов при передаче и разрешен доступ ШКД к сети. Иначе — доставка кадров-запросов повторяется. Тогда, с учетом выражения (2), z -прр интервала обслуживания при передаче кадров-запросов

$$g_{\text{ШКД}}(z) = \frac{Q_{c\text{ШКД}}}{z^C - P_{\text{ШКД}}}, \quad Q_{c\text{ШКД}} = Q_d Q_{k\text{ШКД}} Q_{m\text{ШКД}}, \quad P_{c\text{ШКД}} = 1 - Q_{c\text{ШКД}}; \quad (5)$$

$$Q_{k\text{ШКД}} = (1-p)^{n_{\text{ШКД}}}, \quad Q_{m\text{ШКД}} = (1 - Q_d \Theta_{\text{ШКД}})^{N-1},$$

где $n_{\text{ШКД}}$ — длина кадра-запроса, $\Theta_{\text{ШКД}}$ — вероятность занятости буфера ШКД; z -прр времени задержки при передаче запросов на разрешение сеансов связи определяется формулой (4) с подстановкой в нее выражений (5).

Подсеть УКД. Кадры-ответы от УКД к ШКД считаются обслуженными, если в сообщениях не обнаружено ошибки. Если ошибка обнаружена, доставка кадров-ответов повторяется. С учетом формулы (2) выражение для z -прр интервала обслуживания при передаче кадров-ответов будет иметь вид

$$g_{\text{УКД}}(z) = \frac{Q_{c\text{УКД}}}{z^C - P_{c\text{УКД}}}, \quad Q_{c\text{УКД}} = (1-p)^{n_{\text{УКД}}}, \quad P_{c\text{УКД}} = 1 - Q_{c\text{УКД}}, \quad (6)$$

где $n_{\text{УКД}}$ — длина кадра-ответа; z -прр времени задержки при передаче ответов на запросы определяется формулой (4) с подстановкой в нее выражений (6).

Взаимовлияние подсетей учитывается в системе уравнений интерференции:

$$\left. \begin{aligned} \Theta_{\Pi} &= q_{\text{и}\Pi} \overline{n_{s\Pi}}, \quad \overline{n_{s\Pi}} = (d/dz^{-1})g_{\Pi}(z) \Big|_{z=1}, \quad \Theta_{\Pi} < 1; \\ \Theta_{\text{ШКД}} &= q_{\text{и}\text{ШКД}} \overline{n_{s\text{ШКД}}}, \quad \overline{n_{s\text{ШКД}}} = (d/dz^{-1})g_{\text{ШКД}}(z) \Big|_{z=1}, \quad \Theta_{\text{ШКД}} < 1, \\ \Theta_{\text{УКД}} &= q_{\text{и}\text{УКД}} \overline{n_{s\text{УКД}}}, \quad \overline{n_{s\text{УКД}}} = (d/dz^{-1})g_{\text{УКД}}(z) \Big|_{z=1}, \quad \Theta_{\text{УКД}} < 1. \end{aligned} \right\} \quad (7)$$

Подставив в систему уравнений (7) выражения (3), (5) и (6) и упростив, получим

$$\left. \begin{aligned} \Theta_{\Pi} &= q_{\text{и}\Pi} C Q_{c\Pi}, \quad \Theta_{\Pi} < 1; \\ \Theta_{\text{ШКД}} &= q_{\text{и}\text{ШКД}} C Q_{c\text{ШКД}}, \quad \Theta_{\text{ШКД}} < 1, \\ \Theta_{\text{УКД}} &= q_{\text{и}\text{УКД}} C Q_{c\text{УКД}}, \quad \Theta_{\text{УКД}} < 1. \end{aligned} \right\} \quad (8)$$

Вероятностно-временные характеристики процессов передачи данных. Среднее время задержки при передаче кадров в подсетях можно найти, используя выражения (1)—(8):

$$t_{qi} = \frac{CT_0(2 - q_{\text{и}i}(C+1))}{2(Q_{ci} - Cq_{\text{и}i})}. \quad (9)$$

Приведем выражения для расчета вероятности своевременной доставки кадров всех типов для случая стохастического ограничения на время обслуживания заявок в подсетях, при котором допустимое время обслуживания заявок в подсетях задается геометрическими распределениями с параметрами τ_i :

$$\overline{P_{qi}} = f_{qi}(z) \Big|_{z=\tau_i^{-1}}, \quad \tau_i = 1 - T_0 / \overline{T_{\text{доп}i}}, \quad (10)$$

где $\overline{T_{\text{доп}i}}$ — среднее допустимое время „старения“ кадров, передаваемых в каждой из трех подсетей.

Информационные скорости общего применения (ОП) и реального времени (РВ) рассматриваемых подсетей определяются из следующих выражений:

$$\left. \begin{aligned} R_{сП}^{ОП} &= \lambda_{иП} k_{П} N, \lambda_{иП} = q_{иП} / T_0, R_{сП}^{PB} = R_{сП}^{ОП} \overline{\Pi_{qП}}; \\ R_{сШКД}^{ОП} &= \lambda_{иШКД} k_{ШКД} N, \lambda_{иШКД} = q_{иШКД} / T_0, R_{сШКД}^{PB} = R_{сШКД}^{ОП} \overline{\Pi_{qШКД}}, \\ R_{сУКД}^{ОП} &= \lambda_{иУКД} k_{УКД}, \lambda_{иУКД} = q_{иУКД} / T_0, R_{сУКД}^{PB} = R_{сУКД}^{ОП} \overline{\Pi_{qУКД}}. \end{aligned} \right\} \quad (11)$$

Заключение. Итак, используя выражения (9)—(11), можно произвести численный анализ вероятностно-временных характеристик процессов передачи информации, поступающей от пользователей, и запросов и ответов на разрешение доступа к информационным ресурсам, а также оценить влияние внедрения централизованного устройства контроля доступа на качество передачи информации в сети.

СПИСОК ЛИТЕРАТУРЫ

1. Кожанов Ю. Ф., Колбанёв М. О. Технология инфокоммуникации. Курск: НАУКОМ, 2011.
2. Двухуровневая модель информационного взаимодействия / Б. Я. Советов, М. О. Колбанёв, Т. М. Татарникова // Материалы VIII Санкт-Петербург. межрегион. конф. „Информационная безопасность регионов России“, 23—25 окт. 2013 г. СПб: СПОИСУ, 2013. С. 184—185.
3. Левкин И. М. Информационные проблемы современного общества // Цензура в России: история и современность: Сб. науч. тр. / Под ред. В. Р. Фирсова. СПб: Изд-во „Российская национальная библиотека“, 2013. Вып. 6. С.108—125.
4. Биячуев Т. А. Безопасность корпоративных сетей: Учеб. пособие / Под ред. Л. Г. Осовецкого. СПб: СПбГУ ИТМО, 2004.
5. Доронин А. И. Бизнес-разведка. М.: Ось-89, 2013.
6. Суворов А. А. Архитектура сетей связи с разграничением доступа на основе шлюзов контроля доступа // Материалы конференции „Информационная безопасность регионов России“, 28—30 окт. 2009 г. СПб: СПОИСУ, 2009. С. 140.
7. Верзун Н. А. Модель процесса передачи информации в сети с разграничением прав доступа с использованием устройства контроля доступа // Материалы VIII Санкт-Петербург. межрегион. конф. „Информационная безопасность регионов России“, 23—25 окт. 2013 г. СПб: СПОИСУ, 2013. С. 134.
8. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Оценка вероятности эрланговского старения информации // Информационно-управляющие системы. 2013. № 6. С. 25—28.
9. Чугреев О. С., Македонский М. А. Моделирование локальных информационных систем с услугами административного управления // Междунар. конф. по информационным сетям и системам — ICINAS-2000, 2—7 окт.: Тр. ЛОНИИС. СПб: СПбГУТ, 2000. С. 332—344.
10. Верзун Н. А. Множественный доступ в информационных системах: Учеб. пособие. СПб: СПбГУТ, 2007. 92 с.

Сведения об авторах

- Наталья Аркадьевна Верзун** — канд. техн. наук, доцент; Санкт-Петербургский государственный экономический университет, кафедра прикладных информационных технологий; E-mail: dina_25@hotmail.ru
- Андрей Игоревич Воробьёв** — канд. техн. наук; Санкт-Петербургский государственный экономический университет, кафедра прикладных информационных технологий; E-mail: vorobiov_a@inbox.ru
- Екатерина Дмитриевна Пойманова** — Санкт-Петербургский государственный экономический университет, кафедра прикладных информационных технологий; ассистент; E-mail: e.d.poumanova@gmail.com

Рекомендована кафедрой прикладных информационных технологий

Поступила в редакцию 28.04.14 г.